(U) Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide

(U) Federal Bureau of Investigation

(U) Intelligence Branch

(U) 0579DPG

(U) Published Date: November 06, 2014

(U) Review Date: November 06, 2017

(U) Note: This document incorporates the Policy Directive and the Policy Guide

(U) Revised: 09/29/2015

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

POLICY DIRECTIVE

0579D

1. Policy Directive Title.	(U) Social Media and Other Electronic Information Sharing Technologies
2. Publication Date.	2014-11-06
3. Effective Date.	2014-11-06
4. Review Date.	2017-11-06

5. Primary Strategic Objective.
P5-Information Dissemination and Integration

6. Authorities

6.1. (U) Clinger-Cohen Act of 1996, Title 40 United States Code (U.S.C.) Section (§) 11101 et seq.

6.2. (U) The Privacy Act of 1974, 5 U.S.C. § 552a et seq.

6.3. (U) Federal Records Act of 1950, as amended

6.4. (U) Federal Wiretap Act, 18 U.S.C. § 2510 et seq.

6.5. (U) Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq.

6.6. (U) Freedom of Information Act, 5 U.S.C. § 552

6.7. (U) Federal Information Security Management Act, 44 U.S.C. § 3541 et seq.

6.8. (U) Intelligence Reform and Terrorism Prevention Act of 2004

6.9. (U) Creation and Maintenance of Federal Records, Subpart A: Identifying Federal Records, Title 36 Code of Federal Regulations (CFR) § 1222.20

6.10. (U) Classified National Security Information, 32 CFR Part 2001

6.11. (U) Ethics in Government Act of 1978, 5 U.S.C. App. 101 et seq., and implementing regulations at 5 CFR § 2635, 3801

6.12. (U) National Security, 50 U.S.C. § 401 et seq.

6.13. (U) Executive Order 12968, Access to Classified Information, 1995

6.14. (U) Executive Order 13526, Classified National Security Information, as amended, 2010

6.15. (U) Executive Order 13450, Improving Government Program Performance, 2007

6.16. (U) Executive Order 13556, Controlled Unclassified Information, 2010

6.17. (U) Federal Rules of Criminal Procedure for the United States District Courts 6(e) The Grand Jury; Recording and Disclosing the Proceedings

6.18. (U) Federal Rules of Civil Procedure, rule 26(b)(1)

6.19. (U) Federal Rules of Criminal Procedure, rule 26

6.20. (U) OMB Circular A-130, Management of Federal Information Resources

6.21. (U) Department of Justice Order 2640.F, Information Technology

7. Purpose:

7.1. (U) This policy establishes the Social Media and Other Electronic Information Sharing Technologies Policy Guide (PG) as the overarching FBI authorities on Electronic Information Sharing Technologies (EIST), including:

7.1.1. (U) U.S. Government (USG) EIST, which are under the operational control of a USG entity and open only to USG personnel.

7.1.2. (U) Publicly-available EIST, which are available to the general public whether controlled by the USG or a non-USG entity.

8. Policy Statement:

8.1. (U) The Social Media and Other Electronic Information Sharing Technologies PG enable FBI personnel to effectively and securely share information using EIST while still protecting sources, investigative operations, national security information, and the privacy and civil liberties of US persons.

8.1.1. (U) The Social Media and Other Electronic Information Sharing Technologies PG contains rules and regulations for FBI personnel accessing any EIST for any reason.

8.1.2. (U) The Social Media and Other Electronic Information Sharing Technologies PG also includes technical requirements and content management policies for FBI EIST and official FBI presences on publicly-available EIST.

9. Scope:

(U) The Social Media and Other Electronic Information Sharing Technologies directive and PG applies to all FBI personnel accessing any EIST for any reason including developing, establishing, configuring, managing, maintaining, or operating EIST in the course of their official duties, except as detailed in Section 12.

10. Proponent:

(U) Intelligence Branch

11. Roles and Responsibilities:

(U) All FBI personnel who access any EIST for any reason must adhere to the policies, procedures, and roles and responsibilities set forth in the Social Media and Other Electronic Information Sharing Technologies PG.

12. Exemptions: b7E

(U//~~FOUO~~) This PG does not apply to the [redacted] of EIST. Investigative and operational policies and procedures, including the Domestic Investigations and Operations Guide (DIOG), the Undercover and Sensitive Operations Policy Guide (0432PG), and the National Security Undercover Operations Policy Guide (0307PG) govern the use of EIST in those circumstances.

13. Supersession:

13.1. (U) FBI Policy Directive 0327D, *FBI Participation in Collaborative Environments*, October 6, 2011.

13.2. (U) *Manual of Administrative Operation and Procedures* (MAOP) Part II Section 11-7, "Administrative use of Internet/Internet Electronic Mail (E-Mail) Policy and Guidelines"

13.3. (U) MAOP II Section 11-7.1, "General Information"

13.4. (U) MAOP II Section 11-7.2, "Internet Conduct"

13.5. (U) Electronic communication (EC) 66-HQ-A1196196 serial 61, "Administrative Use of Internet and Email Policy and Guidelines"

13.6. (U) FBI Email Policy (September 2003)

14. References, Key Words, and Links:

14.1. (U) References:

14.1.1. (U) FBI *Operations Security Program Policy* (0196D) and *Operations Security Policy Guide* (0196PG)

14.1.2. (U//~~FOUO~~) FBI *Information System Use Policy* (0071D)

14.1.3. (U) FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form (FD-889);

14.1.4. (U//~~FOUO~~) FBI *Unclassified Network Policy* (UNET Policy v1.0);

14.1.5. (U) *Records Management Policy Guide* (0769PG)

14.1.6. (U//~~FOUO~~) FBI *Security Incident Program (SIP) Policy Directive* (0150D);

14.1.7. (U//~~FOUO~~) *Domestic Investigations and Operations Guide Policy Directive* (0460D) *and Domestic Investigations and Operations Guide Policy Guide*

14.1.8. (U) FBI *Undercover and Sensitive Operations Policy Guide* (0432PG)

14.1.9. (U//~~FOUO~~) (link is to ~~SECRET//NOFORN~~ document) FBI *National Security Undercover Operations Policy Guide* (0307PG)

14.1.10. (U//~~FOUO~~) FBI *Information Sharing Activities with Other Government Agencies Policy* (0012D)

14.1.11. (U) *Prepublication Review Policy Guide*, 0792PG

14.1.12. (U) FBI *Privacy Policy* (0299D) and Privacy Act Rules of Behavior

14.1.13. (U//~~FOUO~~) FBI *Protecting Privacy in the Information Sharing Environment Policy* (0095D)

14.1.14. (U//~~FOUO~~) *Intelligence Program Policy Directive and Policy Guide,* 0718DPG.

14.1.15. (U) *FBI Ethics and Integrity Program Policy Directive and Policy Guide* (0754DPG)

14.1.16. (U) FBI Employment Agreement (FD-291)

14.1.17. (U) FBI *Seal, Name, Initials, and Special Agent Gold Badge Policy Directive* (0266D)

14.1.18. (U) FBI Social Networking Sites and FBI Employee Guidance

14.1.19. (U) FBI OPA *Media Relations at FBIHQ and in Field Offices Policy Guide* (0809PG)

14.1.20. (U) FBI OPA *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet* (0627D)

14.1.21. (U) *Electronic Recordkeeping Certification Policy Guide*, 0800PG

14.1.22. (U) (Link may contain ~~SECRET//NOFORN~~ content) Controlled Access Program Coordination Office

14.1.23. (U) FBI Undercover and Sensitive Operations PG (0432D)

14.2. Key Words:

14.2.1. (U) Electronic Information Sharing Technologies (EIST)

14.2.2. (U) Official use

14.2.3. (U) Personal use

14.2.4. (U) Social media

14.2.5. (U) Social networking

14.3. Links:

14.3.1. (U) FBI Operations Security Program OPSEC (0628D)

14.3.2. (U//~~FOUO~~) FBI Information Systems Use Policy (0581D)

14.3.3. (U) FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form (FD-889)

14.3.4. (U//~~FOUO~~) FBI Unclassified Network Enclave (UNET) Policy (0723D)

14.3.5. (U) *Records Management Policy Guide* (0769PG)

14.3.6. (U//~~FOUO~~) Security Incident Program (0610D)

14.3.7. (U//~~FOUO~~) Domestic Investigations and Operations Guide (0667DPG)

14.3.8. (U) FBI Undercover and Sensitive Operations PG (0432PG)

14.3.9. (U//~~FOUO~~) FBI National Security Undercover Operations PG (0307PG)

(link is to ~~SECRET//NOFORN~~ document)

14.3.10. (U//~~FOUO~~) FBI Information Sharing Activities with Other Government Agencies Policy (0012D)

14.3.11. (U) *Prepublication Review Policy Guide* (0792PG)

14.3.12. (U) FBI *Privacy Policy* (0299D)

14.3.13. (U) FBI Privacy Act Rules of Behavior

14.3.14. (U//~~FOUO~~) FBI Protecting Privacy in the Information Sharing Environment Policy (0095D)

14.3.15. (U) Intelligence Program Policy Directive and Policy Guide (0718DPG)

14.3.16. (U) *FBI Ethics and Integrity Program Policy Directive and Policy Guide* (0754DPG)

14.3.17. (U) FBI Employment Agreement (FD-291)

14.3.18. (U) FBI Seal, Name, Initials, and Special Agent Gold Badge Policy Directive (0625D)

14.3.19. (U) Media Relations at FBIHQ and in Field Offices

14.3.20. (U) *Electronic Recordkeeping Certification Policy Guide*, 0800PG

14.3.21. (U) Controlled Access Program Coordination Office (Link may contain ~~SECRET//NOFORN~~ content)

14.3.22. (U) FBI Undercover and Sensitive Operations PG (0432D)

15. Definitions:

15.1. (U) EIST: Webpage-based tools (including, but not limited to, wikis, blogs, microblogs, photo sharing, personal profiles, social networking sites, dating sites, professional networking sites, and bookmark sharing) and point-to-point communication tools (including, but not limited to, instant messenger, email, direct messages, VOIP, phone calls, and short message service or text messaging). These technologies are used to facilitate the exchange of information in an interactive manner, allowing people to share and discuss information, ideas, activities, events, and interests.

15.1.1. (U) Publicly-Available EIST: Any EIST available to the general public, whether operated by a USG or non-USG entity.

15.1.2. (U) USG EIST: Any EIST under the operational control of a USG entity and not available to the general public.

15.2. (U) FBI Personnel: Any individual employed by, detailed, or assigned to the FBI, including interns; task force officers, members, or participants; members of the Armed Forces; expert consultants; industrial or commercial contractors, licensees, certificate holders, or grantees, including all subcontractors or personal service contractors; or any other person who acts for or on behalf of the FBI, as determined by the FBI Director.

15.3. (U//~~FOUO~~) [redacted] b7E

15.4. (U) Official Use: Activities undertaken by FBI personnel that support the FBI mission, including administrative, agent, and professional staff job functions.

15.5. (U) Personal Use: Activities conducted for purposes other than accomplishing the FBI mission.

15.6. (U) Social networking sites: A webpage-based EIST that enables the discovery, formation, and maintenance of personal and professional relationships. Publicly-available examples include Facebook and LinkedIn; USG examples include Intelink profiles and eChirp.

15.7. (U//~~FOUO~~) Undercover Activities: Any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another federal, state, or local law enforcement organization working with the FBI.

16. Appendices, Attachments, and Forms:

(U) Social Media and Other Electronic Information Sharing Technologies Policy Guide

Sponsoring Executive Approval	
Name:	Kerry Sleeper
Title:	Assistant Director, Directorate of Intelligence
Stakeholder Executive Approval	
Name:	Dean E. Hall
Title:	Associate Executive Assistant Director, Information Technology Branch
Stakeholder Executive Approval	
Name:	Jerome M. Pender
Title:	Executive Assistant Director, Information and Technology Branch
Final Approval	
Name:	Kevin L. Perkins
Title:	Associate Deputy Director

UNCLASSIFIED//~~FOUO~~

(U) Social Media and Other Electronic Information Sharing Technologies Policy Guide

(U) Federal Bureau of Investigation

(U) Intelligence Branch

(U) 0579PG

(U) November 06, 2014

(U) Revised: 09/29/2015

(U) General Information

(U) Questions or comments pertaining to this policy guide can be directed to the Federal Bureau of Investigation Headquarters, Intelligence Branch
(U) Point of contact: chief information sharing officer

(U) Supersession Information

(U) This document supersedes FBI Policy Directive 0327D, *FBI Participation in Collaborative Environments,* dated October 6, 2011; the *Manual of Administrative Operation and Procedures* (MAOP) Part II Section 11-7, "Administrative use of Internet/Internet Electronic Mail (E-Mail) Policy and Guidelines"; MAOP II Section 11-7.1, "General Information"; MAOP II Section 11-7.2, "Internet Conduct"; electronic communication (EC) 66-HQ-A1196196 serial 61, "Administrative Use of Internet and Email Policy and Guidelines"; and the FBI Email Policy (September 2003)

(U) Table of Contents

(U) List of Appendices

1. (U) Introduction

1.1. (U) Purpose and Scope

(U) This policy guide (PG) enables Federal Bureau of Investigation (FBI) personnel to effectively and securely share information using electronic information sharing technologies (EIST) while still protecting sources, investigative operations, national security information, and the privacy and civil liberties of United States (U.S.) persons (USPER). This guidance will afford FBI personnel a greater degree of confidence that they are complying with applicable laws and other FBI and United States government (USG) policies while using EIST.

(U) This PG establishes:

- (U) Responsibilities of FBI components in governing access to, and use of, USG or publicly available EIST by FBI personnel.
- (U) Rules of behavior for FBI personnel accessing and using USG or publicly available EIST, whether for personal or official use, including consequences for misuse.
- (U) Processes for the development, establishment, configuration, management, maintenance, and operation of EIST for official FBI use.

(U) Specific mediums, platforms, and technologies may change over time; however, this PG is intended to address FBI personnel connecting with others using EIST, regardless of such changes.

1.2. (U) Background

(U) EIST are digital communication technologies used to exchange information. The FBI has adopted some EIST to facilitate or improve communications and operations. However, use of any EIST by FBI personnel carries risks to FBI personnel, other parties, and the FBI as a whole. These risks include compromise of sensitive data, critical information, or classified data.

(U) For the purposes of this PG, EIST are defined as technologies used to facilitate the interactive exchange of information that allow people to share, discuss, and collaborate on information, ideas, activities, events, and interests. EIST may take the form of either Web-based tools (e.g., wikis; blogs; tagging; and professional- and social-networking sites) or point-to-point communication tools (e.g., traditional digital and wireless phone calls, Voice over Internet Protocol [VoIP], e-mails, text or short message services, and instant messaging).

(U) In this PG, EIST are divided into two types, based on availability:

1. (U) USG EIST, which are under the operational control of a USG entity and not available to the general public.
2. (U) Publicly available EIST, which are available to the general public, whether operated by a USG or non-USG entity.

(U) EIST are also separated into two usage categories:

1. (U) Official use, which covers the use of EIST to perform job duties and carry out the FBI's mission.
2. (U) Personal use, which is any use of EIST other than to perform mission-related tasks.

1.3. (U) Exemptions

(U//~~FOUO~~) This PG does not apply to the establishment, configuration, and operation of EIST for [redacted] Policies and procedures governing the use of EIST in such investigative or operational situations may be found in: b7E

- (U//~~FOUO~~) The *Domestic Investigations and Operations Guide* (DIOG).
- (U//FOUO) The *Undercover and Sensitive Operations Policy Guide* (0432PG).
- (U//~~FOUO~~) The *National Security Undercover Operations Policy Guide* (0307PG).
- (U//~~FOUO~~) Subsections 3.5.1. and 3.5.2. (inclusive) of the *Confidential Human Source Policy Guide* (0836PG) .

Additionally, specific information regarding the [redacted] of EIST may also be found on the FBI Open Source Program Intranet site. b7E

1.4. (U) Compliance

(U) Failure to comply with this PG or any other applicable policy, rule, law, or regulation in the course of using EIST may result in administrative, disciplinary, civil, or criminal action.

2. (U) Roles and Responsibilities

2.1. (U) FBI Division/Field Office (FO) Heads

(U) FBI Division/FO heads must:

- (U) Ensure division/FO personnel follow the policies and procedures in this PG and other applicable policies when transmitting information on EIST.
- (U) Coordinate with USG EIST systems owners to ensure inappropriate content posted by FBI personnel in divisions/FOs is removed.
- (U) Ensure disciplinary proceedings are initiated to address misuse of USG or publicly available EIST by FBI personnel within their divisions/FOs.
- (U) Provide an annual reminder to FBI personnel in the divisions/FOs that recorded communication transmitted through USG EIST or publicly available EIST accessed from FBI information systems is potentially discoverable in criminal and civil proceedings and that record material created or received using USG EIST must be managed according to policy.
- (U) Act as or designate the FBI system owner for any information system where the division/FO is responsible for the procurement, development, integration, modification, operation and maintenance, or final disposition of the system.
- (U) Seek Office of Public Affairs (OPA) approval to establish new official FBI presences on publicly available EIST. Refer to Corporate Policy Directive (CPD) 0627D. *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*, for further guidance.

2.2. (U) FBI Systems Owners

(U) FBI systems owners must:

- (U) Establish the terms of use for EIST under the system owner's control.
- (U) Grant and revoke user access to USG EIST on FBI information systems under the system owner's control, including:
  - (U) Record requests for user access and restriction.
  - (U) Restrict user access according to mission needs.
  - (U) Ensure user access lists are reviewed and updated at least quarterly.
  - (U) Ensure a process exists to inform new users of restrictions, guidelines, and policies regarding behavior on USG EIST.
- (U) Establish, configure, and operate USG EIST under the system owner's control in accordance with the technical requirements detailed in Section 4 of this PG.
- (U) Establish USG EIST with appropriate access conditions (see subsection 3.2.1.2.1.) on FBI information systems under the system owner's control.

- (U) Designate content managers for Web-based EIST under the system owner's control.
- (U) Develop and implement information retention and disposition procedures, in coordination with FBI content managers, for EIST under the system owner's control, using standards established by the Records Management Division (RMD), the Office of the General Counsel (OGC), or other authority (e.g., legal holds, discovery requirements, and records management policy and guidance).
- (U) Configure and maintain EIST under the system owner's control, in accordance with Section 4 of this PG; PD 0095D, *Protecting Privacy in the Information Sharing Environment*; and other applicable policies.
- (U) Establish and implement procedures to:
  - (U) Identify and remove inappropriate content (including that identified by FBI content managers, Security Division [SecD], or Inspection Division [INSD]) from EIST under the system owner's control.
  - (U) Report inappropriate content to the content manager or appropriate entity to have it removed, unless it is subject to a legal hold in accordance with the PD 0619, *Legal Hold Policy*.
- (U) Document EIST in the system's security documentation for hosting information systems under the system owner's control.
- (U) Coordinate the implementation and monitoring of security controls with SecD.
- (U) Establish and implement audit and review protocols to ensure compliance with this PG.

2.3. (U) FBI Content Managers

(U) FBI content managers must:

- (U) Monitor the content on USG EIST under the content manager's control for compliance with this PG; PD 0095D, *Protecting Privacy in the Information Sharing Environment Policy*; and other applicable policies.
- (U) Remove content that violates this or other applicable policies from USG EIST under the content manager's control when discovered or when requested by the FBI system owner, unless it is subject to a legal hold or security incident investigation. If EIST content is subject to a legal hold, contact OGC's Discovery Coordination and Policy Unit for instruction. Contact SecD's Security Compliance Unit (SCU) regarding security incident investigations.
- (U) Report user violations of this PG on USG EIST under the content manager's control to FBI systems owners for user access revocation, when appropriate, and comply with the reporting requirements of other applicable policies.

- (U) Report security violations on USG EIST under the content manager's control in accordance with the PD 0610D, *Security Incident Program.*
- (U) In coordination with FBI systems owners, develop, implement, enforce, and submit to RMD's Records Automation Section for approval, information retention and disposition procedures for EIST under the content manager's control using the standards established by RMD, OGC, or other authority (e.g., legal holds, discovery requirements, and records management policy and guidance).

  Specifically, content managers must:

  - (U) Manage record materials in accordance with the *Records Management Policy Guide*, 0769PG, dated June 04, 2015 and, if an RMD-authorized recordkeeping system, the *Electronic Recordkeeping Certification Policy Guide*, 0800PG, dated August 14, 2015.
  - (U) Provide FBI personnel with specific instructions for preserving record information created or received using USG EIST under the content manager's control.
  - (U) Manage nonrecord information in accordance with the *Records Management Policy Guide*, 0769PG and other disposition instructions provided by RMD, unless it is subject to a legal hold or other legal requirement.
  - (U) Delete nonrecord point-to-point communications transmitted using USG EIST under the content manager's control after one year, in the absence of a legal requirement to retain information, including copies maintained in back-up storage.
  - (U) Retain any USG EIST content and metadata subject to a legal hold or legal requirement, pursuant to the instructions in the legal hold notice until the conclusion of the hold or release of hold.
- (U) Establish, configure, and operate USG EIST in accordance with the technical requirements detailed in Section 4 of this PG.

2.4. (U) Information Technology Branch (ITB)

(U) ITB must:

- (U) Support the timely identification and preservation of record information (or any data or metadata, whether record or nonrecord, subject to a legal hold) created or received by EIST on FBI information systems, through the development and deployment of tools, as appropriate.
- (U) Support FBI systems owners with configuring and maintaining EIST on FBI information systems, as appropriate.

2.5. (U) Security Division

(U) SecD must:

- (U) Provide security awareness training and operational security guidance to FBI personnel on the use, for any reason, of any USG EIST or publicly available EIST.
- (U) Review and investigate responses on the FD-981, "FBI Report of Foreign Contacts" (available via the Enterprise Process Automation System [EPAS]); the SF-86, "Questionnaire for National Security Positions"; the personnel security interview (PSI); and other background investigations for suspicious EIST encounters.
- (U) Monitor access and use of publicly available EIST from FBI information systems, and prohibit access as necessary.
- (U) Review and investigate reported security violations on USG EIST or publicly available EIST.
- (U) Review and act on requests for exemptions to the security requirements in subsections 3.1.2.; 3.3.2.; 3.3.3.; 4.2. (item 2); and 4.4.1. of this PG regarding the development or use of EIST on FBI information systems.
- (U) Respond to OPA, when asked, regarding official FBI presences on, or contributions to, publicly available EIST as appropriate.
- (U) Coordinate with FBI systems owners for the implementation and monitoring of security controls (e.g., malicious software or data detection methodologies requiring portion marking, access control, and consent to monitoring warnings).
- (U) Communicate information technology threats affecting EIST to FBI systems owners.
- (U) Coordinate with FBI division/FO heads and USG EIST systems owners to remove content posted on EIST by FBI personnel that is in violation of security policies.
- (U) Enforce the security requirements in subsections 3.1.2.; 3.3.2.; 3.3.3.; 4.2. (item 2); and 4.4.1. of this PG through FBI security programs.

2.6. (U) Office of Public Affairs

(U) OPA must:

- (U) Authorize FBI personnel to speak on behalf of the FBI by using any media, including posting content on official FBI presences and publicly available EIST, in accordance with the *Media Relations at FBIHQ and in Field Offices Policy Guide*, 0809PG and other public affairs policies.
- (U) Serve as the FBI system owner and FBI content manager for all official FBI presences on publicly available EIST that are not exempt from CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*.

- (U) Review and approve or reject requests to create new official FBI presences on publicly available EIST.
- (U) Manage nonexempt official FBI presences on publicly available EIST, in compliance with this PG; CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*, and other applicable policies.
- (U) Oversee all official FBI presences on publicly available EIST to ensure they comply with applicable FBI, Department of Justice (DOJ), and USG policies, regulations, and federal laws.
- (U) Refer to CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*, for specific OPA roles and responsibilities regarding the use, establishment, configuration, and operation of publicly available EIST.

2.7. (U) Records Management Division

(U) RMD must:

- (U) Provide guidance to FBI personnel on how to determine whether material transmitted using any USG EIST or publicly available EIST is a federal record.
- (U) Provide record retention and disposition guidance to FBI systems owners, FBI content managers, and FBI personnel.
- (U) Enforce the records management configuration requirements set forth in Section 4 of this PG.
- (U) Make approval decisions regarding records management procedures developed by FBI content managers.

2.8. (U) Office of the General Counsel

(U) OGC must:

- (U) Notify systems owners and responsible FBI personnel and entities of the scope and duration of legal holds, preservation and discovery requirements, or other retention periods affecting USG EIST.
- (U) Provide instructions to content managers regarding the handling of USG EIST content that is subject to a legal hold through the Discovery Coordination and Policy Unit.
- (U) Manage and maintain all recordkeeping requirements associated with legal holds on content obtained from USG EIST.
- (U) Issue policy and guidance regarding the handling, sharing, and protecting of personally identifiable information (PII) through the Privacy and Civil Liberties Unit.
- (U) Enforce the legal configuration requirements in found in Section 4 of this PG.

- (U) Review and provide OPA with decisions on requests for memoranda of understanding (MOU) with publicly available EIST providers.

2.9. (U) Inspection Division

(U) INSD must review and act on misuse of USG EIST and publicly available EIST by employees, as reported by SecD, systems owners, content managers, division/FO heads, and supervisors.

2.10. (U) Case Agents

(U) Case agents must review, act on, and document requests from FBI personnel to disseminate case-related information, including information that may become the subject of testimony (i.e., FD-302s), via EIST, when required.

2.11. (U) Chief Security Officers (CSO)/Information Systems Security Officers (ISSO)

(U) CSOs and ISSOs must:

- (U) Review, through the FD-981 (available via EPAS), reports of foreign and suspicious contacts acquired through USG or publicly available EIST in accordance with PD 0446D, *Official Foreign Contacts*, and PD 0535D, *Unofficial Contacts and Reporting Requirements*.
- (U) Review exemption requests for transmitting FBI information on publicly available EIST in the course of personal use, and refer to SecD for approval decisions. See subsection 3.3.3. of this PG for more information on exemption requests.
- (U) Assess the effectiveness of security controls for tracking user activity, classification marking of content, and software assurance through a continuous monitoring strategy.
- (U) Employ malicious software or data detection methodologies per the applicable incident response plan.

2.12. (U) Supervisors

(U) FBI supervisors must:

- (U) Provide guidance to FBI personnel on the use of USG EIST and publicly available EIST, as needed.
- (U) Refer subordinates' suspected misuse of USG EIST to systems owners for user access termination or other appropriate action.
- (U) Refer subordinates' suspected misuse of USG and publicly available EIST to INSD for appropriate action.

2.13. (U) FBI Personnel

(U) FBI personnel must:

- (U) Follow applicable laws and FBI, DOJ, and USG policies, rules, and regulations including, but not limited to, those listed in this PG when using USG EIST for personal or professional use or publicly available EIST for professional use.
- (U) Comply with the terms of use for USG EIST and publicly available EIST accessed from FBI information systems, unless the terms of use have been superseded by an MOU or related terms of agreement with the FBI.
- (U) Never download or install software or applications from USG EIST or publicly available EIST on FBI information systems.
- (U) Report known or suspected incidents of information spillage, disclosure of USG protected information (USGPI) (including PII and other sensitive information), or other security violations on USG EIST and publicly available EIST in accordance with PD 0610D, *Security Incident Program*, and the *Information Spillage Policy Guide* (0655PG-2), as applicable.
- (U) Determine whether information transmitted using USG EIST and publicly available EIST constitutes a record, and preserve all record information transmitted using EIST in accordance with FBI records management policies and specific instructions established by RMD, OGC, or other authorities.
- (U) Report non-security-related inappropriate content transmitted by FBI personnel on USG EIST to the appropriate FBI supervisor.
- (U) Coordinate with the responsible case agent before transmitting case-related information on USG EIST if in doubt of the operational or information security risk of sharing that information.
- (U) Follow applicable dissemination procedures when using USG EIST, including procedures for protected information.
- (U) Disclose personal use of EIST during background investigations, including on any related forms or during any interviews.
- (U) Report suspicious contacts acquired through USG EIST or publicly available EIST to the CSO, and disclose known or suspected reportable foreign contacts acquired through USG EIST or publicly available EIST on the FD-981, "FBI Report of Foreign Contacts" (available via EPAS).
- (U) Document and submit requests for transmitting nonexempt information on publicly available EIST to the CSO for review. (See subsection 3.3.3. of this PG for more information on exemption requests.)

3. (U) Processes and Procedures for EIST Users

(U) Policies regarding the use of EIST varies with the type of EIST used and why the EIST is being used. The following links provide direct navigation to the policy statements that apply to each use. See Appendix D of this PG for a quick reference guide.

- (U) Use of All EIST
- (U) Official Use of EIST
  - (U) Official Use of USG EIST
  - (U) Official Use of Publicly Available EIST
- (U) Personal Use of EIST
  - (U) Personal Use of USG EIST
  - (U) Personal Use of Publicly Available EIST from FBI Information Systems
  - (U) Personal Use of Publicly Available EIST from Personal Electronic Devices

3.1. (U) Use of All EIST

3.1.1. (U) General

(U) FBI personnel must follow applicable laws and FBI, DOJ, and USG policies, rules, and regulations when using any EIST. This PG is not an exhaustive list of every regulation pertaining to EIST; therefore, FBI personnel must, when in doubt, use discretion and ask a supervisor for additional guidance about acceptable use of any EIST.
(U) FBI personnel using FBI information systems to access EIST that have terms of use must follow the terms of use, unless they have been superseded by an MOU or related terms of agreement with the FBI.

3.1.2. (U) Security Requirements for EIST Users

(U) FBI personnel must take measures to protect classified and sensitive information when using any EIST. Refer to PD 0628D, *FBI Operations Security Program (OPSEC)*; PD 0632D, *Safeguarding Classified National Security Information*; and the *Safeguarding Classified National Security Information Policy Guide* (0632PG) for guidance on how to properly protect FBI information assets.
(U) EIST must not be used to transmit information that exceeds the classification level of the information system where the EIST is located or accessed. Additionally, Sensitive Compartmented Information must only be transmitted on EIST cleared for Sensitive Compartmented Information in the same compartment(s).
(U) Information on any EIST that does not have correct classification or dissemination markings or is unsuitable for distribution on the EIST must be reported in accordance with PD 0610D, *Security Incident Program*. This includes any suspected cases of spillage, contamination, or inadvertent disclosure.
(U) FBI personnel using FBI information systems in an official or personal capacity to access any EIST must:

- (U) Abide by PD 0581D, *FBI Information System Use Policy*; the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form"; and, when using UNet, PD 0723D, *Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy*.
- (U) Protect USG-protected information (USGPI) – including personally identifiable information (PII) – from unauthorized disclosure.
- (U) Never download or install unauthorized software or applications from EIST, unless specifically authorized to do so.

3.2. (U) Official Use of EIST

3.2.1. (U) Official Use of USG EIST

(U) When using USG EIST, FBI personnel must comply with:

- (U) The guidance, policies, and established terms of use of the EIST they are accessing.
- (U) The guidance and policies of the hosting agency, including guidance on classifications and proper sourcing.
- (U) Technical and security requirements for that EIST.

3.2.1.1. (U) Records Management Requirements

(U) Information exchanged on USG or publicly available EIST during the conduct of official duties may constitute record material, even though the EIST may not be an approved FBI recordkeeping system. In accordance with the *Records Management Policy Guide*, 0769PG, dated June 04, 2015, FBI personnel must enter all information that meets the definition of a federal record, including data and metadata created or received using EIST, into an RMD-authorized recordkeeping system.
(U) Point-to-point communications transmitted on USG EIST that do not constitute a record must only be retained for a maximum of one year, if the content is technologically capable of being retained. The one-year limit may only be superseded by a legal requirement (e.g., a legal hold). Any data or metadata on USG EIST that is subject to a legal hold must be handled in accordance with PD 0619D, *Legal Hold Policy*.

3.2.1.2. (U) Guidelines for Transmitting Information

(U//~~FOUO~~) Information may be transmitted on USG EIST in accordance with the access conditions of the tool (see subsection 3.2.1.2.1.); the dissemination controls and handling caveats of the information (see subsection 3.2.1.2.2.); PD 0012D, *FBI Information Sharing Activities with Other Government Agencies*; and applicable policies.
(U//~~FOUO~~) The FBI encourages information sharing with federal agencies and other partners; however, FBI personnel must exercise discretion when sharing information on USG EIST in all circumstances and must seek supervisory input as needed.

3.2.1.2.1. (U) Access Conditions

(U) Before transmitting any information via USG EIST, FBI personnel must first determine what users are authorized to access the EIST, according to the following access conditions:

1. (U) Unrestricted access – any USG EIST that permits access without verifying that users have a mission need to view the information.
2. (U) Controlled access – any USG EIST that can only be accessed by users with a mission need to receive the information and who are properly cleared to receive such information, which may include users from other federal agencies, local law enforcement, etc.
3. (U) Controlled access (FBI-only users) – any USG EIST that can only be accessed by FBI personnel with a mission need to receive the information and who are properly cleared to receive such information.

3.2.1.2.2. (U) Information Dissemination Controls and Handling Caveats

(U) Although the FBI encourages information sharing, certain types of information must be restricted for legal or security purposes. When using USG EIST, FBI personnel must follow the same restrictions that govern information sharing in the physical world, including laws, executive orders (EO), regulations, the DIOG, and other applicable policies and rules, including guidelines on protecting sources and methods.
(U) The following chart provides examples of some common categories of information and what kind of USG EIST may be used to transmit the information.

(U)

	Unrestricted Access	**Controlled Access**	**Controlled Access (FBI-Only Users)**
	USG EIST that permits access without verifying that users have a mission need to view the information	USG EIST that can only be accessed by users with a mission need to receive the information and who are properly cleared	USG EIST that can only be accessed by FBI personnel with a mission need to receive the information and who are properly cleared
Category 1 Information that may be transmitted on USG EIST with unrestricted access	Y	Y	Y
Category 2 Information that may only be transmitted on USG EIST with controlled access	N	Y	Y
Category 3 Information that may only be transmitted on USG EIST with controlled access and that may only be accessed by FBI personnel	N	N	Y
Category 4 Information that must not be transmitted on any EIST	N	N	N

3.2.1.2.2.1. (U) Information Transmittable on USG EIST with Unrestricted Access

(U) Category 1 includes information that may be transmitted on USG EIST with unrestricted access. This category includes, but is not limited to:

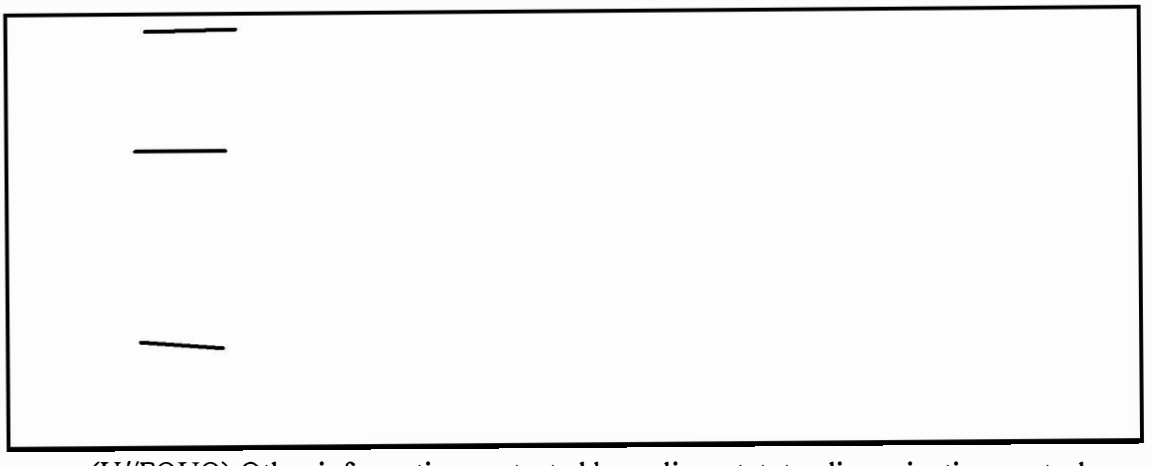
- (U) Information released through official FBI statements and press releases.
- (U) Information approved through the RMD prepublication review process, as outlined in the *Prepublication Review Policy Guide*, 0792PG, dated June 04, 2015.
- (U) Publicly available information on the official duties of Senior Executive Service (SES) personnel regarding titles, official responsibilities, and employment biographies.
- (U) Information free from dissemination controls, handling caveats, or other sensitive content that makes it improper to release in an open environment.

3.2.1.2.2.2. (U//~~FOUO~~) Information Transmittable on USG EIST with Controlled Access

(U//~~FOUO~~) Category 2 includes information that may only be transmitted on USG EIST with controlled access. This category includes, but is not limited to:

[redacted] b7E

- (U//~~FOUO~~) USPER information, including PII. Note that all PII disclosures must be in accordance with the *Privacy Policy Guide* (0299PG); the "Privacy Act Rules of Behavior"; and PD 0095D, *Protecting Privacy in the Information Sharing Environment Policy*, including any requirement for legal review prior to dissemination outside the DOJ.
- (U//~~FOUO~~) Information marked Dissemination and Extraction of Information Controlled by Originator (ORCON), portion marking (OC).
- (U//~~FOUO~~) Federal grand jury/Rule 6(e). Note that access to federal grand jury information may only be granted to those on the 6(e) list.
- (U//~~FOUO~~) Information that may be subject to discovery, including information covered by the Jencks Act, Title 18 United States Code (U.S.C.) Section (§) 3500; *Brady v. Maryland,* 373 U.S. 83 (1963); *Giglio v. United States,* 405 U.S. 150 (1972); or Rule 16. If discoverable material is created in the course of using USG EIST, it must be appropriately documented.
- (U//~~FOUO~~) Title III information pertaining to foreign intelligence; counterintelligence; and to prevent or respond to a threat of a potential or actual attack or a grave hostile act.
- (U//~~FOUO~~) Draft material with "DRAFT, DELIBERATIVE PROCESS PRIVILEGED DOCUMENT" clearly marked on it.



b7E

- (U//~~FOUO~~) Other information protected by policy, statute, dissemination control, or handling caveat that restricts its dissemination to this category.

3.2.1.2.2.3. (U//~~FOUO~~) Information Transmittable on USG EIST with Controlled Access and Only Accessible by FBI Personnel

(U//~~FOUO~~) Category 3 includes information that may only be transmitted on USG EIST with controlled access and that may only be accessed by FBI personnel. This category includes, but is not limited to:

- (U//~~FOUO~~) Case-related information of a sufficiently singular nature, including, but not limited to:
  - (U//~~FOUO~~) Information that would compromise a specific investigation if disseminated.
  - (U//~~FOUO~~) Information regarding operational activities.
  - (U//~~FOUO~~) Information that is automatically or manually restricted in the FBI's central recordkeeping system (i.e., Sentinel).

  (U//~~FOUO~~) Caveat: Any dissemination of case-related information, including that shared on USG EIST, must be approved by the case agent and shared in accordance with DIOG Section 14, "Retention and Sharing of Information."
- (U//~~FOUO~~) Sensitive data concerning electronic devices and techniques.
- (U//~~FOUO~~) Information requiring legal review prior to disclosure.
- (U//~~FOUO~~) Information solely for FBI internal use.
- (U//~~FOUO~~) Sensitive procurement information, including acquisition-sensitive information, such as contractor bid and proposal, proprietary, or source selection information.
- (U//~~FOUO~~) Privileged attorney-client communications or attorney work product.
- (U//~~FOUO~~) Title III information relevant to a specific investigation or official duty.

- (U//~~FOUO~~) Other information protected by any policy, statute, dissemination control, or handling caveat that restricts its dissemination to this category.

3.2.1.2.2.4. (U//~~FOUO~~) Information Prohibited from Transmission on Any EIST

(U//~~FOUO~~) Category 4 includes information that must not be transmitted on any EIST including, but not limited to, other information protected by any court order, policy, statute, dissemination control, or handling caveat that restricts its dissemination to this category.

3.2.2. (U) Official Use of Publicly Available EIST

(U) Official use of publicly available EIST is restricted to public relations purposes and certain operational activities. Provided below is guidance regarding the use of publicly available EIST for both types of circumstances.

3.2.2.1. (U) Public Relations

(U) OPA is the system owner and content manager for all official FBI presences on publicly available EIST that are not exempt from CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*. Only personnel authorized by OPA to speak on behalf of the FBI may post content for public relations purposes on official FBI presences. See PD 509D, *Media Relations at FBIHQ and in Field Offices*, for further instruction.

3.2.2.2. (U) Operational Activities

[redacted] b7E

the FBI at any time (see subsection 1.3). Refer to DIOG subsections 18.5.1 and 18.5.4 for additional instruction regarding the use of these techniques.

3.3. (U) Personal Use of EIST

3.3.1. (U) Personal Use of USG EIST

(U) Personal use of USG EIST is permitted only when a minimal personal use exception (i.e., no interference with official business, negligible cost to the government, and no prohibited activities) is applicable, as described in *FBI Ethics and Integrity Program Policy Directive and Policy Guide*, 0754DPG.

(U) Any nonrecord information generated or received on USG EIST in the course of personal use must only be retained for a maximum of one year. The one-year limit may only be superseded by a legal requirement (e.g., a legal hold). Any data or metadata on USG EIST that is subject to a legal hold must be retained until the conclusion of the hold or release of the hold, pursuant to the instructions in the legal hold notice.

3.3.2. (U) Personal Use of Publicly Available EIST from FBI Information Systems

(U) Additional restrictions apply to personal use of publicly available EIST from FBI information systems. Minimal personal use of publicly available EIST from FBI information systems is permitted in accordance with the *FBI Ethics and Integrity Program Policy Directive and Policy Guide*, 0754DPG. SecD has prohibited the personal use of the following publicly available EIST on FBI information systems at any time and reserves the right to prohibit other such EIST, as circumstances dictate:

- (U) Social-networking sites
- (U) Non-USG instant messenger or chat
- (U) Photo-sharing sites
- (U) Any EIST that requires the installation of unapproved software on an FBI information system
- (U) Sites that contain sexually explicit material, contraband, or other material considered inappropriate for viewing in the workplace
- (U) Sites that may cause network congestion or delays in conducting official business (e.g., sites involving the downloading of large files and photos)
- (U) Sites that involve political activities prohibited in the federal workplace
- (U) Sites that may result in infringements to any copyright, patent, trademark, trade secret, or other proprietary rights of third parties

3.3.3. (U) Personal Use of Publicly Available EIST from Personal Electronic Devices

(U) When accessing publicly available EIST for personal use, FBI personnel are entitled to and retain their constitutional rights, including their freedom to comment on matters of public interest.[1] However, FBI personnel must balance this right with their obligation to protect FBI information at all times. Therefore, when accessing publicly available EIST for personal use, FBI personnel must:

- (U) Comply with the FD-291, "FBI Employment Agreement," and the *Prepublication Review Policy Guide*, 0792PG, dated June 04, 2015, when disclosing FBI-related information, either during or after service with the FBI.

[1] (U) The Hatch Act prohibits federal employees from engaging in political activities while they are on duty or in a federal workplace, including those that make use of any EIST. FBI employees are further restricted from engaging in political activity on behalf of, or in concert with, a political party, partisan political group, or candidate for partisan public office, including those that make use of EIST. For example, FBI employees are prohibited from posting or linking to campaign material or the website or social media profile of a partisan political party, candidate, or political group. Refer to the U.S. Office of Special Counsel memorandum dated April 4, 2012, titled "Frequently Asked Questions Regarding Social Media and the Hatch Act," for additional guidance concerning the Hatch Act's application to social media or other EIST activity.

- (U) Comply with PD 0625D, *FBI Seal, Name, Initials, and Special Agent Gold Badge*, when using the FBI seal, name, initials, or the special agent gold badge on publicly available EIST.
- (U) Be candid regarding the use of publicly available EIST on the SF-86, "Questionnaire for National Security Positions," during a PSI and during any other background or security investigation.
- (U) Complete an FD-981, "FBI Report of Foreign Contacts," for all reportable foreign contacts acquired through publicly available EIST.
- (U) Be familiar with the operational security guidance in the *Social Networking Sites and FBI Employee Guidance* booklet.

(U) Additionally, when accessing publicly available EIST for personal use, FBI personnel must not:

- (U) Disclose any information in violation of the FD-291, "FBI Employment Agreement," without official written authorization by the FBI, including the disclosure of information from, or related to, FBI files or any other information acquired by virtue of official employment.
- (U) Imply or claim that they are speaking on behalf of the FBI, the DOJ, or the USG.
- (U) Display photographs or videos of other FBI personnel if the disclosure would reveal the individuals' FBI affiliation, unless the individuals have expressly consented to the use of such photographs or videos or unless the information has been publicly released in an authorized fashion.
- (U) Display photographs or videos involving official FBI-related matters or FBI facilities without approval from the facility's CSO, unless the information has been publicly released in an authorized fashion.
- (U) Establish a publicly available EIST that appears or claims to be an official FBI presence or affiliated with the FBI.
- (U) Enter, register, document, use, or associate official FBI e-mail addresses in user profiles of personal publicly available EIST.

(U) Exemption requests for posting other types of FBI information on publicly available EIST during personal use must be submitted to the CSO for review, then to the assistant director (AD), SecD (or designee) for a decision. However, the following types of FBI information may be disclosed on publicly available EIST without additional approvals:

- (U) Information and related graphics released through official FBI statements and press releases or disclosed in accordance with the *Media Relations at FBIHQ and in Field Offices* Policy Guide, 0809PG and other applicable OPA policies.
- (U) Publicly available information on the official duties of SES personnel regarding titles, official responsibilities, and employment biographies.

- (U) Information approved through the RMD prepublication review process, as outlined in the *Prepublication Review Policy Guide*, 0792PG, dated June 04, 2015.
- (U) Résumés containing no USGPI or information with the potential to reveal FBI operations.

4. (U) Technical Requirements for Establishing, Configuring, and Operating EIST

4.1. (U) Establishment of EIST on FBI Information Systems

(U) An FBI division/FO head who wishes to establish EIST on an FBI information system must submit a request to the FBI system owner. FBI systems owners establish EIST on FBI information systems under their control.
(U) An FBI system owner must designate an FBI content manager for all Web-based EIST established on FBI information systems under the system owner's control.
(U) An FBI content manager must:

- (U) Monitor content on EIST under the content manager's control and remove content that violates this or other applicable policies, when discovered, or when requested by the FBI system owner, unless the content is subject to a legal hold.
- (U) Develop, implement, and enforce procedures for retaining and destroying EIST content in accordance with information retention and disposition standards (e.g., legal holds discovery requirements, records management policy and guidance) established by RMD, OGC, or other authorities.
- (U) Report EIST user violations of this PG to FBI system owners, when appropriate.

(U) Exemptions: Exemption requests regarding the development or use of EIST on FBI information systems must be directed to FBI systems owners and must be submitted in writing to SecD.

4.2. (U) Establishment of Official FBI Presences on Publicly Available EIST

(U) All official FBI presences on publicly available EIST must be approved by OPA prior to their establishment. This approval requirement includes Web-based EIST, such as social-networking sites and any publicly available EIST established in partnership with other government agencies or private sector organizations.

(U) To establish a new official FBI presence on publicly available EIST, a requestor must submit a business case to OPA's FBI.gov and Internet Operations Unit. For more information on creating new official FBI presences on publicly available EIST, see CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet.*

4.2.1. .(U) Exemptions

(U) Exemption requests regarding the development or use of publicly available EIST must be submitted in writing to OPA. Specific exemptions include the following:

- (U) Official FBI presences on publicly available EIST are exempt from the requirements for display of the highest classification of information allowed and classification portion markings.

- (U) Official FBI presences on publicly available EIST used to collect information on suspected crime or criminal activities are exempt from the requirement for user registration and authentication.

4.3. (U) Configuration of EIST

(U) EIST on FBI information systems and official FBI presences on publicly available EIST must be configured to meet FBI and federal requirements for:

- (U) OPA media guidelines and public affairs policies for OPA approval procedures and procedures on establishing a new official FBI presence on publicly available EIST. (See CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*).
- (U) Security, including, but not limited to:
  - (U) Tracking user activities.
  - (U) Classification marking.
  - (U) Software assurance security.
  - (U) Auditing.
  - (U) Incident response plans (IRP).
- (U) Records management, including compliance with the *Electronic Recordkeeping Certification Policy Guide*, 0800PG, dated August 14, 2015, if the EIST is an RMD-authorized recordkeeping system. Records management procedures for EIST on FBI information systems must be developed in collaboration with RMD and are subject to RMD approval.
- (U) Human oversight and management of posted content.

4.4. (U) Configuration of FBI Information Systems Used to Host EIST

(U) FBI information systems used to host EIST must be developed, established, configured, managed, maintained, and operated in a manner that follows security, legal, and records management requirements.

4.4.1. (U) Security Requirements

(U) FBI information systems used to host EIST must:

- (U) Protect USGPI.
- (U) Ensure the confidentiality, integrity, and availability of information on the information system.
- (U) Display a banner (solid color matching the 700 series standard forms) indicating the most restrictive classification and dissemination controls permitted on the information system.
- (U) Require portion marking to be applied according to requirements in the Controlled Access Program Coordination Office's *Intelligence Community*

Authorized Classification and Control Markings Register and Manual, EO 13526, and Title 32 Code of Federal Regulations (CFR) Parts 2001 and 2003.

- (U) Separate, physically or logically, official FBI presences on EIST that are available to the public through the Internet from FBI administrative and operational networks.
- (U) Employ malicious software or data detection methodologies per the applicable IRP.
- (U) Require registration, authentication, and acknowledgement of terms of use prior to use.
- (U) Employ an interactive feature that requires the user to consent to FBI monitoring and agree that the user has no expectation of privacy while using the system.
- (U) Document all EIST in the information system's security documentation.

(U) Violation of the information system security requirements is justification for review of the security authorization to operate of an FBI information system hosting EIST.

4.4.2. (U) Legal Requirements

(U) FBI information systems used to host EIST:

- (U) Must not create privacy issues involving the collection, disclosure, and posting of PII without the concurrence of OGC.
- (U) Must follow the *Privacy Policy Guide* (0299PG).
- (U) Must provide guidelines for posting proprietary information and intellectual property.

4.4.3. (U) Records Management Requirements

(U) FBI information systems used to host EIST must meet records management requirements in accordance with the *Records Management Policy Guide*, 0769PG, and, if an RMD-authorized recordkeeping system, the *Electronic Recordkeeping Certification Policy Guide*, 0800PG.

(U) Information exchanged on EIST may constitute record material, even though the EIST may not be an approved FBI recordkeeping system. In accordance with the *Records Management Policy Guide*, 0769PG, FBI personnel must enter all information that meets the definition of a federal transitory or nontransitory record, including data and metadata created or received using EIST, into an RMD-authorized recordkeeping system.

5. (U) Summary of Legal Authorities

- (U) Freedom of Information Act, 5 U.S.C. § 552
- (U) Privacy Act of 1974, 5 U.S.C. § 552a et seq.
- (U) Federal Wiretap Act, 18 U.S.C. § 2510 et seq.
- (U) Jencks Act, 18 U.S.C. § 3500
- (U) Clinger-Cohen Act of 1996, 40 U.S.C. § 11101 et seq.
- (U) Federal Information Security Management Act, 44 U.S.C. § 3541 et seq.
- (U) National Security Act of 1949, 50 U.S.C. § 401 et seq.
- (U) Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 et seq.
- (U) Federal Records Act of 1950, as amended
- (U) Intelligence Reform and Terrorism Prevention Act of 2004
- (U) Ethics in Government Act of 1978, 5 U.S.C. App. § 101 et seq., and implementing regulations at 5 CFR Parts 2635 and 3801
- (U) Classified National Security Information, 32 CFR Part 2001
- (U) Creation and Maintenance of Federal Records, subpart A: Identifying Federal Records, 36 CFR § 1222.20
- (U) EO 12968, *Access to Classified Information* (1995)
- (U) EO13450, *Improving Government Program Performance* (2007)
- (U) EO13526, *Classified National Security Information*, as amended (2010)
- (U) EO13556, *Controlled Unclassified Information* (2010)
- (U) *Brady v. Maryland*, 373 U.S. 83 (1963)
- (U) *Giglio v. United States*, 405 U.S. 150 (1972)
- (U) Federal Rules of Criminal Procedure, Rule 26 – Taking Testimony
- (U) Federal Rules of Civil Procedure, Rule 26(b)(1) – Duty to Disclose; General Provisions Governing Discovery; Scope in General
- (U) Federal Rules of Criminal Procedure, Rule 6(e) – The Grand Jury; Recording and Disclosing the Proceedings
- (U) Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- (U) Department of Justice Order 2640.2F, *Information Technology*
- (U) Deputy Attorney General memorandum dated March 24, 2014, " Guidance on the Personal Use of Social Media by Department Employees"

Appendix A: (U) Sources of Additional Information

A.1. (U) Applicable Policies and Other Guidance

- (U) *Confidential Human Source Policy Guide* (0836PG) [links to a ~~SECRET//NOFORN~~ document]
- (U) CPD 0672D, *Creating and Maintaining FBI Public Websites and FBI Web Presences on the Internet*
- (U) *Domestic Investigations and Operations Guide*
- (U) *Electronic Recordkeeping Certification Policy Guide*, 0800PG, dated August 14, 2015
- (U) *FBI Ethics and Integrity Program Policy Directive and Policy Guide* (0754DPG)
- (U) PD 0012D, *FBI Information Sharing Activities with Other Government Agencies*
- (U) PD 0581D, *FBI Information System Use Policy*
- (U) PD 0628D, *FBI Operations Security Program (OPSEC)*
- (U) PD 0625D, *FBI Seal, Name, Initials, and Special Agent Gold Badge*
- (U) PD 0723D, *Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy*
- (U) U.S. Office of Special Counsel, "Frequently Asked Questions Regarding Social Media and the Hatch Act"
- (U) *Information Spillage Policy Guide* (0655PG-2)
- (U) *Intelligence Community Authorized Classification and Control Markings Register and Manual*, Version 6.0 [document is U//~~FOUO~~]
- (U//~~FOUO~~) *Intelligence Program Policy Directive and Policy Guide*, 0718DPG
- (U) *Intelligence Information Reports Policy Directive and Policy Guide* (0691DPG)
- (U) PD 0619D, *Legal Hold Policy*
- (U//~~FOUO~~) *Legal Review of Intelligence Information Reports Policy Directive and Policy Guide* (0752DPG)
- (U) *Media Relations at FBIHQ and in Field Offices Policy Guide*, 0809PG
- (U) *National Security Undercover Operations Policy Guide* (0307PG) [links to a ~~SECRET//NOFORN~~ document]
- (U) PD 0466D, *Official Foreign Contacts*
- (U) *Prepublication Review Policy Guide*, 0792PG, dated June 04, 2015

- (U) *Privacy Policy Guide* (0299PG)
- (U) PD 0095D, *Protecting Privacy in the Information Sharing Environment Policy*
- (U) *Records Management Policy Guide,* 0769PG, dated June 04, 2015
- (U) *Safeguarding Classified National Security Information Directive and Policy Guide* (0632DPG)
- (U) PD 0610D, *Security Incident Program*
- (U) *Social Networking Sites and FBI Employee Guidance* booklet
- (U) *Undercover and Sensitive Operations Policy Guide* (0432PG)
- (U) PD 0535D, *Unofficial Contacts and Reporting Requirements* [document is U//~~FOUO~~]

A.2. **(U) Applicable Forms**

- (U) FD-291, "FBI Employment Agreement"
- (U) FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form"
- (U) FD-981, "FBI Report of Foreign Contacts" (available via EPAS)
- (U) "Privacy Act Rules of Behavior"
- (U) SF-86, "Questionnaire for National Security Positions"

A.3. **(U) Intranet Sites for Additional Guidance**

- (U) Controlled Access Program Coordination Office (site is ~~S//NF~~)
- (U) Records Automation Section
- (U) Discovery Coordination and Policy Unit
- (U) FBI.gov and Internet Operations Unit
- (U) FBI Open Source Program
- (U) Privacy and Civil Liberties Unit
- (U) Security Compliance Unit

Appendix B: (U) Contact Information

This table is U//~~FOUO~~.

Information Sharing Policy Board	J. Edgar Hoover Building Room 11079-O 935 Pennsylvania Avenue, NW Washington, DC 20535
Chief Information Sharing Officer	

b6
b7C

Appendix C: (U) Key Words and Acronyms

C.1. (U) Key Words

(U) 700 series standard forms: USG forms and labels used to identify security classification levels or sensitivity of information. These forms are color-coded for easy recognition:

Green	UNCLASSIFIED
Blue	CONFIDENTIAL
Red	SECRET
Orange	TOP SECRET
Yellow	Sensitive Compartmented Information

(U) Access conditions: the restrictions (e.g., user access lists) used to control access to a USG EIST. For the purpose of this PG, the following access conditions apply:

1. (U) Unrestricted access – any USG EIST that permits access without verifying that users have a mission need to view the information.
2. (U) Controlled access – any USG EIST that can only be accessed by users with a mission need to receive the information and who are properly cleared to receive such information. This may include users from other federal agencies, local law enforcement, etc.
3. (U) Controlled access (FBI-only users) – any USG EIST that can only be accessed by FBI personnel with a mission need to receive the information and who are properly cleared to receive such information.

(U) Authorization to operate: a decision that an information system meets security and records management requirements and that the information system may therefore be accredited to become operational.

(U) Blog and microblog: a Website designed to support personal commentary that is open to viewing, comments, and discussion by others. The difference between a blog and a microblog is the amount of content allowed in a single post.

(U) Case-related information: includes reports (whether to a colleague, supervisor, or prosecutor) about investigative activities, characterizations of the merits of particular evidence or potential testimony, evaluations of witness credibility, interactions with witnesses or victims, and any other material potentially subject to discovery.

(U) Classification portion marking: designating parts of a document or Web page (e.g., paragraphs, subparagraphs, titles, subjects, graphics, tables, and appendices) to indicate the classification level or handling caveat applicable to that section.

(U) Content manager: the person or organization with administrative access to all content on a specific EIST. Content managers have the authority to remove content found in violation of this PG or any applicable policy, rule, law, or regulation, as directed by the system owner or other authority (e.g., SecD or INSD).

(U//~~FOUO~~) Critical information:

b7E

(U) Data: a representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by human beings or by automatic means.
(U) Discovery: providing information and materials that may be relevant to requests related to administrative investigations, civil or criminal lawsuits, or other legal matters initiated or reasonably anticipated. Generally, discovery consists of evidence or information that can be used by a defendant to make a conviction less likely or a lower sentence more likely or evidence or information that can be used by a defendant to impeach a key government witness. See the Jencks Act, 18 U.S.C. § 3500; *Brady v. Maryland,* 373 U.S. 83 (1963); and *Giglio v. United States,* 405 U.S. 150 (1972).

(U) Disposition instructions: those actions taken regarding federal records after the records are no longer required to conduct current agency business. These actions include:

- (U) Transfer of records by RMD to agency storage facilities.
- (U) Transfer of permanent records to the National Archives and Records Administration.
- (U) Disposal of temporary records, usually by destruction, authorized by RMD.

(U) Division/FO heads: Ads in headquarters divisions and special agents in charge (SAC) or assistant directors in charge (ADIC) in field offices.
(U) EIST: technologies used to facilitate the interactive exchange of information that allow people to share, discuss, and collaborate on information, ideas, activities, events, and interests. EIST may take the form of Web-based tools or point-to-point communication tools.

- (U) Web-based tool: an application that is accessed over a network connection, and which often runs inside a Web browser. Specific types of Web-based tools include, but are not limited to:
    - (U) Social-networking services (e.g., Google+, Facebook, LinkedIn, Instagram).
    - (U) Social-bookmarking or tagging services (e.g., Pinterest, Reddit, StumbleUpon).
    - (U) Online community services (e.g., Wikipedia, Twitter, Tumblr, and, in general, blogs, microblogs, chat rooms, Internet forums, and virtual discussion groups).
- (U) Point-to-point communication tool: a communication connection between two end points that occurs through a variety of electronic media. Specific types of point-to-point communication tools and the media over which they are used include, but are not limited to:
    - (U) Internet (e.g., e-mail, instant messaging, and VoIP).
    - (U) Radio frequency (e.g., wireless or mobile telephony, text or short message service, multimedia message service, and two-way radio).
    - (U) Fiber optics (e.g., traditional digital telephony).

(U) External dissemination: the formal release of a document or similar material to external entities as an official FBI product.
(U) FBI information: investigative or administrative USGPI used to conduct or support the FBI's mission, and for which the FBI is responsible for providing the controls to generate, collect, process, disseminate, and destroy or dispose of the information.
(U) FBI information system: a discrete set of information resources (e.g., data, hardware, or software) organized for the acquisition, collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of FBI information. [Source: Derived from Committee on National Security Systems Instruction No. 4009]
(U) FBI personnel: persons employed by, or detailed to, the FBI; persons contracted to perform work on behalf of the FBI; persons assigned to FBI-sponsored task forces; persons serving as FBI interns or fellows; persons working under FBI supervision and control, as established by an executed MOU or a memorandum of agreement (MOA); persons who work for a government agency (including the armed forces) and whose access to FBI information systems is specifically defined in, and subject to, FBI supervision and control, as established by an executed MOU, an MOA, a memorandum of instruction, or other appropriate documentation approved by OGC.
(U) Federal record: see "Record."
(U) Handling caveats and dissemination controls: information protected by particular legal requirements for handling and disseminating to ensure proper sharing.
(U) Hyperlink or link: an electronic pointer or reference to a resource at another location.
(U) Inappropriate content: information transmitted via EIST that violates any applicable law or FBI, DOJ, or USG policy, rule, or regulation.
(U) Instant messaging: a technology that creates real-time, text-based communication between two or more participants using the Internet or an internal network.
(U) Intellectual property: products of the human intellect that are documented to record an idea or concept, and which the legal system protects against unauthorized use by others.
(U) Internet: a publicly maintained computer network that can be accessed by FBI personnel or the general public.
(U) Intranet: a privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it. Intranets may be limited to a single organization or to a group of organizations.
(U) Information system: a discrete set of information resources (e.g., data, hardware, software) organized for the acquisition, collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. [Source: Derived from Committee on National Security Systems Instruction No. 4009]
(U) Legal hold: a mandate to preserve potentially relevant or substantive materials pertaining to a discovery request. The hold requires the information to be preserved in its original format with no changes made to the data or metadata.
(U) Memorandum of understanding or terms of agreement: a legal agreement formalizing cooperation between two parties participating in a project.

(U) Metadata: data that describes other data (e.g., a data dictionary contains a collection of metadata).
(U) Microblog: see "Blog."
(U//~~FOUO~~) [redacted] b7E

(U) Network: information systems implemented with a collection of interconnected components that can exchange data or information.
(U) Official FBI presence: a publicly available EIST that OPA has approved for the dissemination of FBI information.
(U) Official use: activities undertaken by FBI personnel that support the FBI mission, including administrative, special agent, and professional staff job functions.
(U) Operational security: a systematic process to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified information on the planning and execution of sensitive activities.
(U) Personal use: activities conducted for purposes other than accomplishing the FBI mission.
(U) Personally identifiable information: a type of USGPI that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
(U) Proprietary information: any financial, business, scientific, technical, economic, or engineering information where the owner has taken reasonable measures to keep the information secret, and the information derives actual or potential economic value from not being public. This information requires protection from unauthorized use and disclosure.
(U) Publicly available: information that has been published or broadcast for public consumption; is available on request to the public; is accessible online or otherwise to the public; is available to the public by subscription or purchase; can be seen or heard by any casual observer; is made available at a meeting open to the public; or is obtained by visiting any place or attending any event that is open to the public.
(U) Publicly available EIST: any EIST available to the general public, whether operated by a USG or non-USG entity.
(U) Record (as defined by 44 U.S.C. § 3301): "… all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them…"

- **(U) Non-record**: any material recorded, made, or received *via Web-based or point-to-point communication tools* during the course of federal business *that has no documentary or evidentiary value to the organization* (e.g., routine informal administrative communications, copies of publications, and electronic versions of blank forms).

- **(U) Non-transitory record**: any material recorded, made, or received *via Web-based or point-to-point communication tools* during the course of federal business *that is needed for longer than 180 days and provides substantive documentation* of the organization's policies and actions, contains important or valuable evidentiary information, or is required to be maintained by law or regulation. In this context, "non-transitory record" and "record" are synonymous.
- **(U) Transitory record**: any material recorded, made, or received *via Web-based or point-to-point communication tools* during the course of federal business and is of *minimal or short-term (180 days or less) documentary or evidentiary value to the organization* (e.g., routine requests for information or publications, quasi-official notices, and documentation of routine activities).
- **(U) Recordkeeping system**: a manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

(U) Reportable foreign contact: contact with foreign nationals is reportable under the following circumstances:

- (U//~~FOUO~~) Ongoing professional or official relationships or associations that are required in order to perform FBI duties and/or assignments, as described in PD 0466D, *Official Foreign Contacts Policy.*
- (U) A change in a relationship from professional to personal.
- (U) Undue interest about employment.
- (U//~~FOUO~~) Illegal or unauthorized access is sought to classified, sensitive, or proprietary information technology.
- (U//~~FOUO~~) [redacted] b7E

(U) Rule 16 (Federal Rules of Criminal Procedure): information that is subject to disclosure upon request of the defendant. It is applicable to oral statements or other documents in the government's possession.
(U) Security Incident Reporting System: an information system used to report and track actual and potential security incidents.
(U) Sensitive Compartmented Information: a type of classified USGPI concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence (DNI).
(U) Sensitive data: any USGPI, as well as generally unclassified information, on the planning and execution of sensitive activities.
(U) Short message service messaging: a point-to-point communications service that allows the exchange of short text messages between mobile devices.
(U) Social-networking site: a Web-based EIST that enables discovery, formation, and maintenance of personal and professional relationships.

(U) Spillage, contamination, or inadvertent disclosure: security incidents involving the transfer of classified or other USGPI onto an information system not accredited or authorized for the information. In this context, it includes classified information on a public Website.
(U) System owner: the person responsible for the procurement, development, integration, modification, operation and maintenance, or final disposition of an information system.
(U) Terms of use: the terms and conditions for using an EIST, including the purpose of the technology, services provided, community served, system owner, and contact information (also referred to as rules of behavior, comment policy, conditions for use, terms of service, or code of conduct).
(U//~~FOUO~~) Undercover activities: any investigative activities involving the use of assumed names or cover identities by employees of the FBI or other federal, state, or local law enforcement organizations working with the FBI.
(U) User: any individual or system process authorized to access an information system.
(U) USG-protected information: information that meets the standards for national security classification under EO 13526, as amended, and is unclassified information but:

- (U) Is pertinent to the national interests of the United States or to the important interests of entities outside the federal government.
- (U) Requires protection from unauthorized disclosure under law or policy.

(U) USG EIST: any EIST under the operational control of a USG entity and not available to the general public.
(U) Web page: a document or information resource that can be accessed through a Web browser. Web pages may be retrieved from a local computer or from a remote server, which may restrict access to a private network or published pages on the Internet.
(U) Website: a collection of interlinked Web pages residing at the same network location. Websites may be limited to a set of specific users through a subscription, registration, or gateway service, or may allow unrestricted access by the general public.
(U) Wiki: a collection of Web pages that capture knowledge and are designed to enable anyone who accesses it to contribute or modify its content.

C.2. (U) Acronyms and Abbreviations

This table is (U).

AD	assistant director
ADIC	assistant director in charge
PD	policy directive
CSO	chief security officer
DIOG	*Domestic Investigations and Operations Guide*

DOJ	Department of Justice
EIST	electronic information sharing technologies
EO	executive order
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FISA	Foreign Intelligence Surveillance Act
FO	field office
IIR	intelligence information report
INSD	Inspection Division
IRP	incident response plan
ISSO	information systems security officer
ITB	Information and Technology Branch
MOA	memorandum of agreement
MOU	memorandum of understanding
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPSEC	operations security
ORCON	Dissemination and Extraction of Information Controlled by Originator
PG	policy guide
PII	personally identifiable information
PSI	personnel security interview
RMD	Records Management Division

SAC	special agent in charge
SCU	Security Compliance Unit
SecD	Security Division
SES	Senior Executive Service
U.S.	United States
U.S.C.	United States Code
USG	United States government
USGPI	United States government-protected information
USPER	United States person (U.S. person)
VoIP	Voice over Internet Protocol

Appendix D: (U) Quick Reference Guide

This table is (U).

USG EIST	**Official Use**	• Follow the guidance, policies, and terms of use of the USG EIST and the guidance and policies of individual agencies. • Only transmit information in accordance with the access level of the EIST and dissemination controls and handling caveats of the information. Examples: editing a wiki article on a USG site, having a work meeting via webcam or instant messenger, or establishing a forum to discuss a business topic on a SharePoint site located on a USG network.
	Personal Use	• Minimal personal use of USG EIST is permitted in accordance with the *FBI Ethics and Integrity Program Policy Guide*. Examples: sending an instant message on FBINet to a co-worker to schedule lunch, contacting a spouse about childcare using e-mail on an FBI-issued mobile device, or calling a local mechanic from an FBI phone regarding a car repair.
Publicly Available EIST	**Official Use**	• All official FBI presences on publicly available EIST must be approved by OPA. • Information and pictures posted to official FBI presences on publicly available EIST must also appear on FBI.gov Websites. Examples: establishing an official FBI presence on a social-networking site, setting up an FBI Website that accepts tips from the public, or sharing official FBI information with the public.
	Personal Use	• Only USG information preapproved for public dissemination may be shared on publicly available EIST. • FBI personnel must be candid about their use of EIST in background and security investigations. • Some publicly available EIST are prohibited for personal use on FBI information systems due to security concerns. Examples: using a public social-networking site for a personal account, posting pictures on a photo-sharing site, or using a personal e-mail account.

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
POLICY DIRECTIVE

0723D

1. Policy Directive Title.	Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy
2. Publication Date.	2014-10-27
3. Effective Date.	2014-10-27
4. Review Date.	2017-10-27

5. Primary Strategic Objective.
T7-Deploy technology and science to make our workforce more effective and efficient.

6. Authorities:

6.1. Title 40 United States Code (U.S.C.) Section (§) 11101(3), Clinger-Cohen Act of 1996, et seq.

6.2. E-Government Act of 2002, U.S.C. Chapter 36

6.3. Office of Management and Budget (OMB) Memorandum M-11-29, Chief Information Officer (CIO) Authorities, dated 08/08/2011

6.4. Department of Justice (DOJ) Memorandum, Guidance on the Personal Use of Social Media by Department Employees, dated 03/24/2014

6.5. DOJ Order 2880.1C, Information Resource Management Program, dated 05/20/2011

6.6. DOJ Order 2740.1A (Change 1), Use and Monitoring of DOJ Computers and Computer Systems, dated 11/30/2010

7. Purpose:

7.1. The Federal Bureau of Investigation's (FBI) mission of intelligence, counterintelligence, counterterrorism, and law enforcement (LE) operations requires a modern, resilient, agile, and secure information technology (IT) infrastructure. The FBI's IT capabilities are rapidly evolving to modernize and improve the effectiveness of the FBI's operational and administrative functions.

7.2. The FBI Unclassified Network (UNet) enclave is an UNCLASSIFIED information system (IS) designed to provide the FBI with mission-essential secure high-speed access to the public Internet. The UNet enclave also provides access to UNCLASSIFIED open sources of information, and provides users with electronic mail (e-mail) capabilities accessed through UNCLASSIFIED workstations, FBI-owned UNCLASSIFIED mobile devices, and Outlook Web Access (OWA).

7.3. This directive establishes requirements for the access, use, management, and maintenance of the UNet enclave. All FBI personnel must refer to relevant security and records management policies (see subsection 14.1.) for further requirements on the use of any FBI IS, security incident reporting, and records management procedures. All personnel are reminded that use of the UNet enclave may be monitored and communications preserved to meet legal requirements, ethics, compliance, and security purposes.

8. Policy Statement:

8.1. Authorized Use of the UNet Enclave by FBI Personnel

8.1.1. The UNet enclave, to include UNet servers and any UNet-hosted device (i.e., mobile devices), is authorized for use to create, view, transmit, receive, store, or process UNCLASSIFIED official United States (U.S.) Government (USG) information.

8.1.2. The UNet is an Internet access system associated with the USG and FBI, and it should not be used for covert or other investigations where anonymity is required unless proper software or systems (e.g., [redacted] are utilized. b7E

8.1.3. The UNet enclave may be used to conduct UNCLASSIFIED investigations, when association with the USG and FBI is not a concern.

8.1.4. Limited personal use of the UNet enclave (e.g., web browsing and accessing personal web-based e-mail) is permitted in accordance with existing regulations (e.g., DOJ Order 2740.01A) regarding the use of government property.

b6
b7C
b7E

[redacted]

8.2. Prohibited Use of the UNet Enclave by FBI Personnel

8.2.1. Except when authorized for official purposes, users are strictly prohibited from using the UNet enclave for the following purposes:

8.2.1.1. To access instant messaging servers and chat rooms (e.g., Gchat and AIM).

8.2.1.2. To access pornographic material.

8.2.1.3. To access gaming and gambling sites.

8.2.1.4. To download or install applications from the Internet (except as otherwise noted in subsection 8.5.5.3.).

8.2.1.5. For peer-to-peer applications (e.g., BitTorrent and LimeWire).

8.2.1.6. For computer-to-computer applications (e.g., PC Anywhere and GoToMyPC), computer-to-phone connections (e.g., Connect Me and GoToMyPC), and other voice-over Internet Protocol services (e.g., Skype and Vonage).

8.2.1.7. Downloading external webmail.

8.2.1.8. Conducting government business using personal e-mail.

8.2.1.9. Conducting government business using personal social media accounts.

8.3. Security Management of the UNet Enclave

8.3.1. Any and all passwords must not be maintained on the UNet enclave or in the UNCLASSIFIED workstation.

8.3.2. All FBI personnel using the UNet, including, but not limited to other government agency (OGA) personnel, LE partners, and contractors, must follow established policies and procedures for the FBI's Security Incident Program (SIP).

8.3.3. UNet user accounts, user login IDs, and passwords must not be shared.

8.3.4. Any documents or files containing personally identifiable information (PII) must be stored and maintained in accordance with the Privacy Act of 1974, Domestic Investigations and Operations Guide (DIOG), the FBI Privacy Policy Implementation Guide (0299PG), and applicable security requirements.

8.3.5. The UNet enclave is an information system that is subject to the provisions and reporting requirements contained within the Federal Information Security Management Act (FISMA) of 2002.

8.4. Policy Statements Specific to the UNet Enclave Customers or Users

8.4.1. Users must not use stand-up servers to host, connect to, or otherwise interact with the UNet enclave system and servers without prior authorization from the Technical Configuration Control Board (TCCB).

8.4.2. All requests for UNet user accounts must be submitted and approved through the System Access Request System (SARS).

8.4.3. Any and all configuration changes made to the UNet enclave must first be coordinated with, and approved by, the TCCB.

8.4.3.1. Any and all configuration changes that require interruptions to the UNet enclave and its operations (i.e., enclave downtime), must be coordinated with, and approved by, the Change Management Board (CMB).

8.4.3.2. Only IT hardware and software approved by the TCCB are authorized for download or installation on UNCLASSIFIED FBI workstations.

8.4.3.3. Approved hardware and software must only be downloaded or installed on UNCLASSIFIED workstations by system administrators. All antivirus updates and patches must only be downloaded or installed on UNCLASSIFIED workstations by the System Management Support Unit (SMSU) and Vulnerability Compliance Support Unit (VCSU) within IT Infrastructure Division (formerly named IT Services Division).

8.4.3.4. Virtual private network (VPN) connections and remote control applications are authorized, but require prior approval from the TCCB.

8.4.3.5. As promulgated by established security policies (e.g., Policy Directive [PD] 0581D and Policy Guide [PG] 0655PG), configuring the UNet enclave to disable the warning banner, passwords, timed automatic lock-out mechanisms, or any other preventative security measures, is prohibited.

8.4.4. Users experiencing difficulties with the UNet enclave or an UNCLASSIFIED workstation must follow the appropriate Enterprise Operations Center (EOC) procedure for submitting a service ticket. These procedures may be obtained on the EOC's FBI Network Intranet site.

8.4.5. Personnel outside of the Enterprise Messaging and Directory Services Support Unit (EMDSSU) must not create additional local administrator accounts on UNCLASSIFIED workstations or laptops. If site technical support staff require local administrator capabilities to troubleshoot such devices, these site technicians must contact the EMDSSU for assistance. Local administrator rights will be provided on a case-by-case basis, based on the respective business requirements of that site.

b6
b7C
b7E

8.5. Policy Statements specific to the UNet Enclave Service Provider or Administrator

8.5.1. The UNet enclave, to include any and all servers, routers, switches, firewalls, and mobile devices hosted on the UNet enclave, must only be managed and maintained by the IT Infrastructure Division (ITID) and the Criminal Justice Information Services (CJIS) Division.

8.5.2. The coordination of all activities at the program level for the UNet enclave, to include the management of enterprise product deployments, must only be managed by the Service and Contact Section (SCS).

8.5.3. All UNet user accounts must have SARS approval, and:

8.5.3.1. Accounts and passwords must be managed and maintained in accordance with applicable information assurance policies and the UNet system security documentation (see Section 14, "References and Links").

8.5.3.1.1. After [redacted] (i.e., when a UNet user enters the wrong login ID or password), the user's account must automatically be locked (except as otherwise noted in subsection 8.5.5.3.). b7E

8.5.3.1.2. Upon separation of any personnel from the FBI, UNet user accounts must be disabled no later than ten days after the initial date of departure from the FBI, and archived no later than 30 days, thereafter.

8.5.3.1.2.1. All privileged user accounts must be removed upon notification from all administrative groups within the Active Directory.

8.5.3.1.3. Any UNet user accounts that are inactive for 90 days must be disabled, and archived no later than 30 days thereafter (except as otherwise noted in subsection 8.5.5.3.).

8.5.3.1.4. Any UNet user accounts with elevated rights (i.e., privileged users) no longer requiring access to information systems must be disabled upon notification from their supervisors.

8.5.4. Configuring the e-mail exchange server accounts on the UNet enclave to automatically forward FBI e-mail to any personal, other nonfederal government agency, or nongovernment entity e-mail accounts is prohibited.

8.5.5. FBI mobile devices connected to the UNet enclave must:

8.5.5.1. Be authorized only at the UNCLASSIFIED level.

8.5.5.2. Be only connected to the UNet enclave through the mobile device management server operated by the Enclave and Field Support Unit (EFSU), ITID.

8.5.5.3. Be deployed, used, and maintained in accordance with all other applicable FBI policies and procedures (e.g., PD 0256D, PD 0581D, and FD-889b).

9. Scope:

This policy applies to all FBI Headquarters (FBIHQ) branches and divisions, field offices (FO), and legal attaches (Legat).

10. Proponent:

Information and Technology Branch (ITB)

11. Roles and Responsibilities:

11.1. The executive assistant director (EAD), ITB, as FBI CIO and FBI authorizing official, must:

11.1.1. Establish and ensure the implementation of the FBI UNet enclave.

11.1.2. Serve as the final approving authority for any and all information systems, IT, and exceptions to this policy.

11.2. The ITID as Service Providers

11.2.1. The assistant director (AD), ITID, must:

11.2.1.1. Ensure the effective management and administration of the UNet enclave, including, but not limited to, patch management, Section 508 compliance, security management (in coordination with UNet information system security manager (ISSM), and approval decisions for exceptions to this policy.

11.2.1.1.1. Ensure the resources necessary for the administration and implementation of all UNet service and support activities are provided.

11.2.1.1.2. Ensure UNet enclave customers are provided guidance for UNet enclave operations, as needed.

11.2.1.1.3. Establish the Technical Configuration Control Board (TCCB).

11.2.1.1.3.1. Ensure that the TCCB operates in accordance with its charter (see Section 14, "References and Links").

11.2.1.1.4. Establish, manage, administer, and implement the Change Management Board (CMB).

11.2.1.1.4.1. As the CMB Chair, ensure the board operates in accordance with its charter (see References and

b6
b7C
b7E

Links).

11.2.2. The section chief (SC), SCS, ITID, must:

11.2.2.1. Ensure the coordination of all activities at the program level for the UNet enclave, which includes the management of enterprise product deployments.

11.2.2.2. Refer to the AD, ITID any IT investment that fails to adhere to this policy.

11.2.2.3. Review and make recommendations to the AD, ITID for requests for exceptions to this policy.

11.2.3. The unit chief (UC), EFSU, ITID, must:

11.2.3.1. Coordinate activities at the program level for the UNet enclave, which includes the management of enterprise product deployments, as directed by the SC, SCS, ITID.

11.2.3.2. Provide guidance to UNet enclave customers for UNet enclave operations, as needed.

11.2.3.3. Manage, administer, and implement the mobile device management server.

11.2.3.4. Refer to the SC, SCS, ITID, any IT investment that fails to adhere to this policy.

11.2.3.5. Review and make recommendations to the SC, SCS, ITID for requests for exceptions to this policy.

11.2.4. The UC, SMSU, ITID, must:

11.2.4.1. Manage, administer, and implement a vulnerability patch management program in coordination with the VCSU, which includes downloading or installing antivirus updates or other patches on UNCLASSIFIED workstations.

11.2.5. The UC, VCSU, ITID, must:

11.2.5.1. Manage, administer, and implement a vulnerability patch management program in coordination with the SMSU.1

11.2.6. The UC, EMDSSU, ITID, must:

11.2.6.1. Manage, administer, and implement identity and authentication systems for FBI ISs, which includes Active Directory.

11.2.6.1.1. Ensure the management and administration of all service provider activities identified in subsection 8.3.3 of this policy.

11.3 CJIS must:

11.3.1. Operate and maintain the FBI UNet Exchange mailbox servers according to this policy in relation to security, patch management, and compliance support.

11.3.2. Operate and maintain the FBI network connectivity for the UNet enclave to have access to the Internet according to this policy in relation to security, patch management, and compliance support.

11.3.3 Operate and maintain the FBI Trusted Internet Connection (TIC), according to this policy in relation to security, patch management, and compliance support.

11.4. System owners, as UNet enclave customers, must:

11.4.1. Ensure all FBI personnel under their purview are aware of, and adhere to, this policy.

11.4.2. Ensure all UNet accounts are submitted and approved through the System Access Request system.

11.4.3. For all ISs under their purview that communicate with or otherwise connect to the UNet enclave ensure the following:

11.4.3.1. Any configuration changes are coordinated with and approved by the TCCB, and:

11.4.3.1.1. Ensure the UNet ISSM is advised of all planned changes for these systems.

11.4.3.1.2. Document and ensure all configuration changes that require an interruption to the UNet enclave and its operations (i.e., enclave downtime) are coordinated and approved by the CMB.

11.4.3.1.3. Ensure all information required by subsection 8.5.3. of this policy is entered timely and accurately into SARS.

11.4.4. Forward all requests for exceptions to this policy to the UC, EFSU, ITID.

11.5. UNet ISSM must:

11.5.1. Enforce security policies through all phases of the UNet life cycle.

11.5.2. Review and approve the system security documentation, in coordination with the UC, EFSU, ITID.

11.5.3. Assess and evaluate all planned changes to the UNet enclave, which includes the identification and categorization of the risk, vulnerability, and impact of the change to that information system (i.e., its environment and operational needs), and its impact on the UNet enclave. Report all findings to the UC, EFSU.

11.5.4. Review requests for exception to this policy and make recommendations to the UC, EFSU, ITID.

11.6. UNet information systems security officer must:

11.6.1. Respond to reported information technology security incidents for information systems under their purview, as directed by the ESOC.

11.6.1.1. Coordinate incident responses with the ESOC and ISSM, as appropriate.

11.6.2. Monitor all users use of UNet FBI ISs for compliance with the rules of behavior.

11.6.3. Annually verify and validate UNet privileged user accounts.

11.6.4. Monitor the status for security patches and updates of UNet information systems under their purview.

11.6.5. Report noncompliant UNet ISs to the IS owner and ISSM.

11.6.6. Maintain and update the UNet system security documentation, as needed.

11.7. FBI personnel must:

11.7.1. Ensure any actions they perform on the UNet enclave are in accordance with those requirements specified in Section 8 of this policy and any established security and records management policies (e.g., PD 0581D, PD 0610D, and the *Records Management Policy Guide* [0769PG]).

11.7.2. Follow established policies and procedures in PD 610D, *Security Incident Program*.

12. Exemptions:

Any exception requests must be reviewed by the UC, EFSU and forwarded to the EAD, ITB, for approval. All requests impacting the security of the UNet enclave, must be coordinate with the UNet ISSM.

13. Supersession:

FBI Unclassified Network (UNet) Policy (v1.0), dated 04/03/2007.

14. References, Key Words, and Links:

14.1.1. Title 29 U.S.C. § 74(d), The Rehabilitation Act of 1973

14.1.2. Public Law (P.L.) 105-220, Workforce Investment Act of 1998, dated 8/7/1998

14.1.3. Office of Management and Budget (OMB), 25 Point Implementation Plan to Reform Federal Information Technology Management, dated 12/09/2010

14.1.4. OMB Memorandum M-09-02, Information Technology Management Structure and Governance Framework, dated 10/21/2008

14.1.5. OMB Memorandum M-05-23, Improving Information Technology (IT) Project Planning and Execution, dated 08/04/2005

14.1.6. Committee on National Security Systems Instruction (CNSSI), No. 4009, National Information Assurance Glossary, dated 04/26/2010

14.1.7. National Institute of Standards and Technology (NIST), SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, dated 09/2011

14.1.8. NIST, SP 800-53 (rev 4), Recommended Security Controls for Federal Information Systems and Organizations, dated 02/19/2014

14.1.9. NIST, IR 7298 (rev.1), Glossary of Key Information Security Terms, dated 5/31/2013

14.1.10. DOJ Order 1000.2A, Department of Justice Policy for Organizational Management, dated 10/19/1983

14.1.11. DOJ Order 2740.1A (Change 1), Use and Monitoring of DOJ Computers and Computer Systems, dated 11/30/2010

14.1.12. PD 0655D, *Security Assessment and Authorization for FBI Information Systems*, 02/12/2014

14.1.13. PG 0655PG, *Security Assessment and Authorization Policy Guide*

14.1.14. FBI Information Technology Strategic Plan 2010-2015, 07/2009

14.1.15. PD 0581D, *FBI Information Systems Use Policy*, 05/02/2008

14.1.16. FBI FD-889, FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

14.1.17. FBI FD-889a, FBI Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form

14.1.18. FBI Unclassified Network (UNet) System Security Plan

b6
b7C
b7E

14.1.19. Technical Configuration Control Board Charter

14.1.20. Change Management Board Charter

14.1.21. IT Infrastructure Library (ITIL), Glossary and Abbreviations (v1.0), 2011

14.1.22. PG 0769PG, *Records Management Policy Guide*

14.1.23. PD 0610D, *Security Incident Program*, dated 08/05/2013

14.1.24. FBI Ethics and Integrity Program Policy Directive and Policy Guide, 0754DPG

14.1.25. The Privacy Act of 1974, Title 5 United States Code (U.S.C.) Section 552a

14.1.26. FBI *Domestic Investigations and Operations Guide* (DIOG)

14.1.27. PG 0299PG, *Privacy Policy Implementation Guide*, 09/20/2010

14.2. Key Words

14.2.1. Clinger-Cohen Act (CCA)

14.2.2. Change Management Board (CMB)

14.2.3. configuration management

14.2.4. information system (IS)

14.2.5. information technology (IT)

14.2.6. patch management

14.2.7. Technical Configuration Control Board (TCCB)

14.2.8. Unclassified Network (UNet)

14.3. Links

14.3.1. Technical Configuration Control Board Charter

14.3.2. Change Management Board Charter

14.3.3. FBI Information Assurance Policies and Resources

14.3.4. FBI Section 508 Program

14.3.5. Enterprise Operations Center

15. Definitions:

15.1. Access: ability to make use of any IS resource.

15.2. Authorization: access privileges granted to a user, program, or process or the act of granting those privileges.

15.3. Configuration management: a discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

15.4. Disable: action taken on a user account whereby a user no longer is able to access data stored under that user's network or e-mail accounts.

15.5. Enclave: collection of information systems connected by one or more internal networks under the control of a single authority and common security policy (i.e., servers, routers, switches, and circuits). The systems may be structured by physical proximity or by function, independent of location (e.g., FBINet and UNet).

15.6. FBI personnel: any individual employed by, detailed, or assigned to the FBI, including members of the Armed Forces; an expert or consultant to the FBI; an industrial or commercial contractor, licensee, certificate holder, or grantee of the FBI, including all subcontractors; a personal service contractor of the FBI; or any other category or person who acts for, or on behalf of, the FBI, as determined by the FBI Director.

15.7. Hosted device: any IT hardware that interfaces or otherwise connects to the UNet enclave that is not a stand alone IS. Hosted devices include mobile devices (i.e., smart phones and tablets).

15.8. Information system: a discrete set of information resources (e.g., data, hardware, and software) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

15.9. Information technology: any equipment, supplies, services, or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. For purposes of this definition, equipment is considered used by an agency if it is used directly by the agency or by a contractor whose contract with the agency (i) requires its use, or (ii) requires, to a significant extent, its use in the performance of a service or the furnishing of a product. IT includes computers, ancillary equipment, software, firmware and similar

b6
b7C
b7E

procedures, services (including support services), and related resources; but IT does not include any equipment that is acquired by a contractor incidental to a federal contract.

15.10. IT service: a service provided by an IT service provider. An IT service is made up of a combination of information technology, people, and processes.

15.11. Limited personal use: use of the government office equipment by employees during nonwork time is considered to be an "authorized use" of government property. Authority for this policy is cited as 5 U.S.C. § 301, which provides that the head of an executive department or military department may prescribe regulations for the use of its property; and Executive Order (EO) 13011, Federal Information Technology, Section 3(a)(1), which delineates the responsibilities of the Chief Information Office council in providing recommendations to agency heads relating to the management and use of information technology resources. Federal employees are permitted limited use of government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the government. This limited personal use of government office equipment should take place during the employee's nonwork time. Some examples of this privilege to use Government office equipment for nongovernment purposes include checking personal e-mail, web browsing, scheduling a medical appointment, and checking investments or banking activities. Agency officials may apply this policy to contractor personnel, interns, and other nongovernment employees through incorporation by reference in contracts or memorandums of agreement as conditions for using government office equipment and space.

15.12. Lock: to make an account inaccessible by the user.

15.13. Mobile device: nonstationary electronic apparatus with singular or multiple capabilities of processing, storing, and/or transmitting voice, data, video, or photo images.

15.14. Network: information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

15.15. Network access: authorization provided to a user (or process acting on behalf of a user) to access information systems communicating through a network (e.g., local area network, wide area network and the Internet).

15.16. Personally identifiable information: information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, and the like, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name.

15.17. Section 508: a codified set of standards requiring federal agencies ensure all electronic and information technology (EIT) that it develops, procures, maintains or uses to be accessible by persons with disabilities. Section 508 of the Rehabilitation Act of 1973, as amended 29 U.S.C. § 794(d), and the Workforce Investment Act of 1998 (P.L. 105-220) mandate that federal employees with disabilities (e.g., visual, hearing, motor, and speech impairments) be provided access to and use of agency systems and information that is equal or comparable to their nondisabled colleagues.

15.18. Service customer: a recipient of IT services. For the purposes of this policy, service customers are receiving IT services from the IT Services Division concerning authorization, access, and use of the UNet enclave. (Derived from: ITIL, Glossary and Abbreviations [v1.0], 2011)

15.19. Service provider: a provider of IT services. For the purposes of this policy, the IT Services Division is providing IT services concerning authorization, access, and use of the UNet enclave to service customers. (Derived from: ITIL, Glossary and Abbreviations [v1.0], 2011)

15.20. System owner: a broad term referring to anyone who manages the acquisition or development of an IS or places an IS into operation. Within the FBI, the CIO and each Assistant Director (AD) is responsible for the operational management of applications or ISs that directly support his/her business area.

15.21. Technical Configuration Control Board: a chartered group of people responsible for evaluating and approving or rejecting proposed changes to configuration items, and for ensuring implementation of approved changes.

15.22. Trusted Internet connection (TIC): is the trusted gateway for all UNCLASSIFIED communications to and from the open Internet.

15.23. Unauthorized access: any access that violates the stated security policy.

15.24. User: FBI personnel or other individual authorized to access FBI ISs.

16. Appendices, Attachments, and Forms:

None

Sponsoring Executive Approval	
Name:	Jennifer R. Sanchez
Title:	Assistant Director, Information Technology Customer Relations and Management Division

b6
b7C
b7E

7/19/2016

Stakeholder Approval	
Name:	Jerome M. Pender
Title:	Executive Assistant Director, Information and Technology Branch
Final Approval	
Name:	Kevin L. Perkins
Title:	Associate Deputy Director

UNCLASSIFIED

b6
b7C
b7E

7/19/2016